Cassandra Crossing/ Cybersicurezza, Generali e Fantaccini

(531)—Nel mondo della sicurezza informatica tutti sanno tutto di come stanno le cose. Fanno schifo! Come si potrebbe fare per cambiarle?

Cassandra Crossing/ Cybersicurezza, Generali e Fantaccini

Figure 1:

(531)—Nel mondo della sicurezza informatica tutti sanno tutto di come stanno le cose. Fanno schifo! Come si potrebbe fare per cambiarle?

6 febbraio 2023—Anche in questo fine settimana i "Maledetti Hacker" hanno conquistato i telegiornali in prima serata, hanno smosso il Presidente del Consiglio ed hanno fatto passare notti insonni anche ai membri dell'Agenzia per la Cybersicurezza Nazionale (con la "y", e grazie a DataKnightmare per il tormentone!).

Cassandra invece era ignara del tutto. Ha passato il sabato e la domenica mattina sconnessa e senza TV. E quando, la sera, il primo titolone è apparso sul tiggì delle 20:30, chi gli stava accanto gli ha chiesto, a ragione, "Ma che succede?"

Domanda legittima, perché la lettura di 10 minuti di notizie, comunicati e dichiarazioni, anche del Presidente del Consiglio, se sottoposte alla tecnica dell'analisi asimoviana (cfr. "Il ciclo delle Fondazione"), si rivelavano vuoti di qualsiasi contenuto od informazione.

Essendo la suddetta persona dotata della massima autorità sul sottoscritto, egli effettuava una rapida googlatina in giro, e scopriva che un malware specializzato aveva colpito un particolare tipo di server (VMWare ESXi) che, quando esposto su internet e mancante di patch da due

anni, aveva una vulnerabilità, che un ransomware specializzato aveva iniziato a sfruttare. Si noti che il fabbricante l'aveva individuata e subito corretta da, appunto, due anni.

Scopriva pure che il fenomeno era già iniziato 24 ore prima in Francia, dove l'equivalente della ACN In Francia, il locale CERT e l'ANSSI—Agence Nationale de la Sécurité des Systèmes d'Information (anche laggiù con la "y", ma usando parole del vocabolario francese)—avevano diramato un comunicato ordinario e senza ecccessivi allarmismi, che segnalava il fenomeno e le contromisure necessarie.

Si, perché bastava infilare una patch e nulla sarebbe successo.

Ora persino Cassandra sa che patchare un server ESXi non è banale, perché bisognerebbe averne due in load balancing, spostare tutto il carico su uno, spegnere il secondo e patcharlo, e ripetere poi l'operazione a ruoli invertiti, con probabili disservizi per la clientela e notti insonni per i sistemisti. Avere sistemi ridondanti costa un botto, ma serve.

Oppure bisognava aver comprato il modulo software apposito di VMWare per l'applicazione delle patch a caldo, che pare costi non poco, ma di nuovo, evidentemente serve.

Ed in ogni caso, sarebbe stato necessario avere sufficiente personale tecnico per tenere sotto controllo la situazione (in italiano si chiama semplicemente "*gestire i server*"), e nulla di tutto questo sarebbe mai successo. E, se è per quello, nemmeno la maggior parte degli incidenti informatici del passato.

Ora, il fatto che si tratti di server specializzati per la gestione di macchine virtuali può spiegare perché nemmeno i pochissimissimi giornalisti con qualche nozione di informatica abbiano capito niente. E che questo abbia avuto la conseguenza che riottosi professori di sicurezza informatica di università per corrispondenza sono stati messi davanti ad una telecamera e violentati a lungo fino a fargli dire che si, potevano essere stati gli hacker russi.

Per favore, date subito un "maledetto hacker" a questi poveri giornalisti, che ve lo chiedono insistentemente; ne hanno tanto bisogno per non dover capire i fatti e poter parlare d'altro, e non di notizie importanti!

Il fatto che fosse domenica può spiegare perché i media e la politica abbiano ingigantito un problema rilevante ma non straordinario o bloccante. Regione Lazio ed ACEA, ad esempio, sono state tirate giù con molto meno clamore e stracciamento di vesti, eppure è stato un problema con conseguenze a livello nazionale e dell'intera popolazione, durate settimane.

Dopo questa lunga premessa, Cassandra può spiegare e profetizzare.

Se vogliamo fare contenti i media e parlare di "Guerra Contro Gli Hacker Russi", la causa di tutto è una guerra è combattuta con un esercito fatto solo di Generali e qualche Ufficiale. Dove ci sono più generali di squadra aerea che aerei, generali dell'esercito che carri armati. Dove i soldati, non quelli delle forze speciali ma gli umili fantaccini in trincea, sono pochissimi o nessuno, come il soldato Nemecsek ne "***I ragazzi della via Paal".***

Anche i bandi di assunzione dell'ACN con la "y" sono formulati in modo tale che senza una "lettera di presentazione" di una persona "autorevole" non sia possibile nemmeno presentare una domanda, come non è possibile se si è dotati di grande esperienza ma ci sono voluti troppo tempo ed anni per accumularla.

Cassandra, ma anche almeno un centinaio di altre persone della "scena" italiana, potrebbero indicare a chiunque e senza sforzo almeno una ventina di nomi di persone da inserire sia in ruoli di graduati che di truppa (niente generali, per carità). Posto che ovviamente gli fossero offerti inquadramenti e stipendi adeguati (si, è necessario ragionare anche di vile pecunia)

Lo stato li vorrebbe? Pare di no, non sono funzionari, lo stato è abituato ad assumere solo funzionari o pseudo "tecnici" che non vedono l'ora di diventarlo.

Le aziende li vorrebbero? Non sia mai, la sicurezza informatica ed i sistemi informativi ben fatti sono solo costi da tagliare, tanto poi ci sono le polizze assicurative per coprire i danni.

Non c'è nessuna soluzione politica. Non c'è nessuna soluzione tecnica.

Potrebbe funzionare una soluzione legislativa.

Un GSPR sulla falsariga del GDPR o della 626. Una legge che ponga a "priori" la responsabilità delle conseguenze di ogni problema di sicurezza informatica non implementata a carico (anche penale, se c'è dolo) dei vertici degli enti statali e delle aziende private, e che gli possa costare il 4% del fatturato lordo annuo globale.

Altrimenti lo status quo penoso della sicurezza informatica italiana, che tutti conoscono tranne i giornalisti ed i politici, e che è diffuso a livello non solo italiano ma globale, è destinato a durare per sempre.

Tanto, le conseguenze, in termini di disservizi, danni e costi delle conseguenze dei danni, le pagheranno sempre i soliti.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on February 6, 2023.

Canonical link

Exported from Medium on August 27, 2025.